INDIRE ISTITUTO NAZIONALE DOCUMENTAZIONE INNOVAZIONE RICERCA EDUCATIVA

FORMAZIONE

FUTURA

Finanziato dall'Unione europea NextGenerationEU

PNRR ISTRUZIONE LA SCUOLA PER L'ITALIA DI DOMANI

Ministero dell'Istruzione e del Merito

PERSONALE ATA

COLLABORATORI · OPERATORI · ASSISTENTI · TECNICI

INDIRE ISTITUTO NAZIONALE DOCUMENTAZIONE INNOVAZIONE RICERCA EDUCATIVA

FORMAZIONE

FUTURA PNRR ISTRUZIONE LA SCUOLA PER L'ITALIA DI DOMANI

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Istruzione e del Merito

PERSONALE ATA

PROTEGGERE I DISPOSITIVI DIGITALI

COLLABORATORI · OPERATORI · ASSISTENTI · TECNICI

Enrico Basile

1. LA SICUREZZA DIGITALE

1. CHE COS'È
2. GESTIRE DATI PERSONALI
3. MINACCE DIGITALI
4. CREARE PASSWORD SICURE

1. LA SICUREZZA DIGITALE > CHE COS'È

La sicurezza digitale comprende tutte le **azioni** e **tecnologie** che **AIUTANO** a prevenire **accessi non autorizzati**, **danni** ai dispositivi e **perdita** di dati.

PROTEZIONE DEI DATI PERSONALI E SCOLASTICI

TUTELA DEI DISPOSITIVI (PC, TABLET, SMARTPHONE)

DIFESA DA VIRUS, TRUFFE, E ATTACCHI INFORMATICI

1. LA SICUREZZA DIGITALE > GESTIRE I DATI PERSONALI

Gli istituti scolastici gestiscono quotidianamente **dati personali**: **proteggerli** è un obbligo legale, ma anche morale.

DATI SENSIBILI DI STUDENTI E PERSONALE

STRUMENTI CONDIVISI DA PIÙ UTENTI

OBBLIGHI DI LEGGE (GPDR)

1. LA SICUREZZA DIGITALE > MINACCE DIGITALI

Un **clic sbagliato** o una **password debole** possono **COMPROMETTERE** la sicurezza dell'intera rete scolastica.

ACCESSI NON AUTORIZZATI

FURTO O PERDITA DI DISPOSITIVI

PHISHING (EMAIL TRUFFA)

VIRUS E MALWARE

1. LA SICUREZZA DIGITALE > CREARE PASSWORD SICURE

UNA **PASSWORD EFFICACE** DEVE:

INCLUDERE LETTERE MAIUSCOLE, MINUSCOLE, NUMERI E SIMBOLI

AVERE ALMENO 12 CARATTERI

ESSERE UNICA PER OGNI SERVIZIO

2. USO CORRETTO DEI DISPOSITIVI SCOLASTICI

1. MODALITÀ DI UTILIZZO
2. PROTEGGERE IL PC
3. AGGIORNAMENTI DI SISTEMA E BACKUP
4. PERDITA DI UN DISPOSITIVO
5. RICONOSCERE UN DISPOSITIVO INFETTO

2. USO CORRETTO DEI DISPOSITIVI SCOLASTICI > MODALITÀ DI UTILIZZO

EVITARE SITI NON SICURI O NON PERTINENTI

UTILIZZARE SOLO I DISPOSITIVI ASSEGNATI

NON INSTALLARE PROGRAMMI NON AUTORIZZATI

NON PRESTARE ACCOUNT O PASSWORD

2. USO CORRETTO DEI DISPOSITIVI SCOLASTICI > PROTEGGERE IL PC

BLOCCARE IL PC (PREMERE I TASTI WINDOWS + L, OPPURE CTRL+ALT+DEL)

NON USARE CHIAVETTE **USB** SCONOSCIUTE

2. USO CORRETTO DEI DISPOSITIVI SCOLASTICI > AGGIORNAMENTI DI SISTEMA E BACKUP

Mantenere il **Sistema Operativo** ed i **software** sempre **aggiornati** per correggere vulnerabilità che potrebbero essere sfruttate dagli *hacker*.

Effettuare spesso **copie di backup** uilizzando soluzioni come **Google Drive** o dischi esterni protetti da password.

2. USO CORRETTO DEI DISPOSITIVI SCOLASTICI > PERDITA DI UN DISPOSITIVO

In caso di **smarrimento** o **furto**:

- **avvisare** tempestivamente l'amministrazione o il tecnico IT
- **cambiare** le password associate
- **bloccare** da remoto il dispositivo, se possibile

2. USO CORRETTO DEI DISPOSITIVI SCOLASTICI > RICONOSCERE UN DISPOSITIVO INFETTO

SEGNALI COMUNI

- Rallentamenti improvvisi e prolungati
- Popup insoliti o frequenti
- L'homepage appare modificata
- Blocchi del sistema senza attività intensa
- Processi o applicazioni sconosciute
- Antivirus disattivati
- Email inviate senza autorizzazione
- Applicazioni o file sconosciuti (malware)

3. STRUMENTI DIGITALI SICURI A SCUOLA

1. IL GPDR
2. STRUMENTI AUTORIZZATI
3. IL REFERENTE IT

3. STRUMENTI DIGITALI SICURI A SCUOLA > IL GPDR

«IL GDPR NON È SOLO UNA LEGGE EUROPEA, MA UNA GARANZIA PER LA RISERVATEZZA DI STUDENTI, FAMIGLIE E PERSONALE. TUTTI DOBBIAMO RISPETTARLO.»

GENERAL DATA PROTECTION REGULATION

3. STRUMENTI DIGITALI SICURI A SCUOLA > STRUMENTI AUTORIZZATI

- Usare solo **piattaforme** e **software** approvati dalla scuola.
- Evitare l'uso di email personali per scopi lavorativi.
- Seguire le linee guida dell'istituto.

IN CASO DI DUBBI O PROBLEMI, RIVOLGERSI AL REFERENTE INFORMATICO: COLLABORARE È IL MODO MIGLIORE PER PREVENIRE DANNI.

CONCLUSIONI

- NON LASCIARE DISPOSITIVI ACCESI E INCUSTODITI
- EVITA DI INSTALLARE PROGRAMMI NON AUTORIZZATI
- SEGNALA IMMEDIATAMENTE SMARRIMENTI O MALFUNZIONAMENTI
- USA SOLO RETI WI-FI SCOLASTICHE UFFICIALI
- PARTECIPA A CORSI DI AGGIORNAMENTO SULLA SICUREZZA DIGITALE, SE PROPOSTI

BIBLIO-SITOGRAFIA

1. Garante per la protezione dei dati personali. (2021). *Scuola e privacy: Vademecum*. https://www.garanteprivacy.it
2. Cert-AgID. (2023). *Linee guida per la sicurezza informatica nelle pubbliche amministrazioni*. Agenzia per l'Italia Digitale. https://www.cert-agid.gov.it
3. NortonLifeLock. (2020). *Cybersecurity per tutti: Come proteggere i dispositivi personali e professionali*. Milano: Apogeo Education.
4. Bocchi, F., & Gervasi, O. (2021). *Sicurezza informatica: Principi di base per utenti comuni*. Roma: Carocci.
5. AgID. (2020). *Linee guida per la sicurezza ICT delle Pubbliche Amministrazioni*. Agenzia per l'Italia Digitale. https://www.agid.gov.it
6. Ghirardini, B. (2021). *Protezione dei dati personali: privacy e sicurezza nei contesti educativi*. FrancoAngeli.
7. Schiavo, F. (2020). *Cybersecurity e protezione dei dati: guida operativa per la scuola digitale*. Hoepli.